Testiranje standardne AND ćelije otporne na bočne napade

Milena Stanojlović, Vančo Litovski, Predrag Petković, *Member, IEEE*

Apstrakt—U ovom radu biće predstavljeni rezultati testiranja NSDDL AND ćelije (No Short-circuit current Dynamic Differential Logic) koja je deo biblioteke ćelija otpornih na napade preko sporednih kanala. Rečnik defekata biće kreiran na osnovu ponovljenih simulacija za svaki defekt, koji se posebno unosi u kolo. Verifikacija će pokazati stepen ranjivosti ćelije u prisustvu defekta. Ispitivaće se uticaj defekata, tipa prekid i kratak spoj, na logičku funkciju kola kao i struju napajanja. Ćelija je projektovana u CMOS TSMC035 tehnologiji korišćenjem Mentor Graphics alata.

***Ključne reči* — CMOS; NSDDL metod; bočni napad; projektovanje; testiranje; kratak spoj; prekid.**

I. UVOD

Domen istraživanja ovog rada je testiranje ćelije projektovane primenom kriptografskog metoda, u hardveru, otpornog na napade preko bočnih (sporednih) kanala (*Side Channel Attack* – SCA) [1].

Pod bočnim napadom podrazumeva se svaki pokušaj neovlašćenog otkrivanja sadržaja šifrovane poruke koji je zasnovan na merenju fizičkih parametara u kriptografskom sistemu. Kao fizički parametri mogu se izdvojiti elektromagnetno zračenje, potrošnja energije, talasni oblici signala kao i ostale veličine i fenomeni koji mogu da pomognu dešifrovanje kripto ključa. Praktično u ovaj skup ulaze svi merljivi fizički fenomeni čija analiza pomaže potencijalnom napadaču da otkrije sadržaj zaštićenih informacija. Uobičajen je termin da informacije "otiču kroz bočne kanale". Jedan od osnovnih izvora curenja informacija iz integrisanih kriptografskih sistema prouzrokuje korelacija između talasnih oblika struje napajanja i aktivnosti integrisanog kola. Zato je razvijeno više metoda koji imaju za cilj da ujednače promenu struje napajanja tako što će je učiniti nezavisnom od promene logičkih stanja u digitalnom kolu .

Posmatranjem dinamike potrošnje elektronskog kripto-sistema može se doći do dodatnih informacija o radu sistema čime se olakšava razotkrivanje šifre. Najefikasniji metodi napada na kripto-sistem jesu SPA (Simple Power Analysis), DPA (Differential Power Analysis) i EMA (Electromagnetic Analysis) [2-3]

Milena Stanojlović – Inovacioni centar naprednih tehnologija, Vojvode Mišića 58/2, 18000 Niš, Srbija (e-mail: milena.stanojlovic@icnt.rs).

Vančo Litovski – Elektronski fakultet, Univerzitet u Nišu, Aleksandra Medvedeva 14, 18000 Niš, Srbija (e-mail: vanco.litovski@elfak.ni.ac.rs).

Predrag Petković – Elektronski fakultet, Univerzitet u Nišu, Aleksandra Medvedeva 14, 18000 Niš, Srbija, (e-mail: predrag.petkovic@elfak.ni.ac.rs).

Promena struje napajanja (I_{DD}) predstavlja veoma važan dodatni izvor informacija o ponašanju kriptografskog sistema. Do nagle promene I_{DD} dolazi u CMOS kolima samo prilikom promene logičkih stanja. Tokom promena sa 0 na 1, pune se izlazne kapacitivnosti od V_{DD} preko PMOS mreže. Pri promenama stanja sa 1 na 0 one se prazne prema masi preko NMOS mreže. Ovome treba dodati i struje "kratkog spoja" tokom intervala u kome vode i PMOS i NMOS tranzistori. Napadaču su poznati pobudni podaci, ali ne može da pristupi tačkama u kojima bi mogao da registruje odziv. Jedini izvor informacija o ponašanju kola jeste aktivnost izražena kroz promenu struje napajanja. Ipak i sama informacija o potrošnji kola u korelaciji je sa aktivnošću kola tako da omogućava brže otkrivanje kriptografskog ključa. U cilju odbrane od curenja informacija, nakon dužeg proučavanja, odabran je metod koji se primenjuje pogodnim projektovanjem hardvera. NSDDL (No Short-circuit current Dynamic Differential Logic) [4] je jedan od metoda za zaštitu podataka koji uspešno sakriva korelaciju između potrošnje i aktivnosti kola.

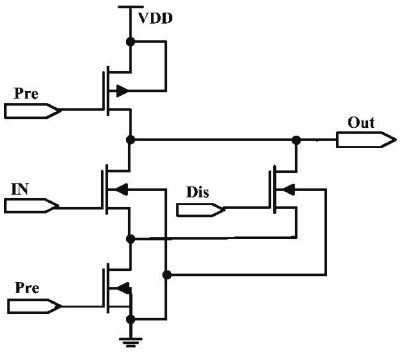
Dalje u radu, posebna pažnja biće posvećena testiranju AND ćelije koja je projektovana po pravilima pomenutog metoda. Namernim uvodjenjem defekata kratkih spojeva i prekida u ispravno kolo pratiće se izlazni signal kao i struja napajanja, za svaki defekt zasebno, pri istim kombinacijama ulaznih signala [5]. Broj simulacija zavisiće od broja defekata koji se testiraju. Rezultati simulacije dobijeni su korišćenjem ELDO simulatora u okviru Mentor Graphics Design Architect alata. Izabrana tehnologija za projektovanje je TSMC035u.

II. METOD ODBRANE OD BOČNIH NAPADA

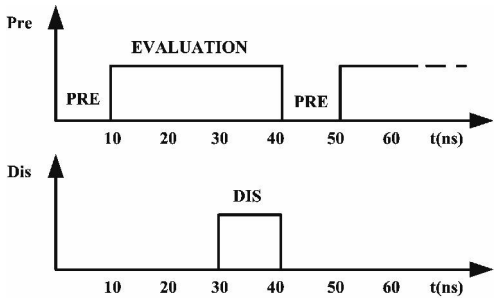
Odabrani NSDDL metod zasnovan je na logici koja se od standardnih razlikuje u dva važna detalja. Najpre, udvojena je hardverska struktura time što se osnovnom kolu paralelno pridružuje kolo koje obavlja komplementarnu funkciju. U slučaju NAND funkcije to je NOR (naravno i obrnuto). Kao rezultat dobija se složena logička ćelija koja sadrži udvostručeni broj ulaznih i izlaznih portova. Pri tome jednom setu ulaznih portova dovode se željeni talasni oblici, dok se drugi pobuđuje komplementarnim signalima. Shodno tome na jednom izlaznom portu generiše se prava vrednost signala, a na drugom lažna – komplementarna. Druga razlika odnosi se na vremenski dijagram generisanja odziva. Za razliku od standardnih kombinacionih logičkih kola, odziv se dobija u tri faze. To su pripremna faza tokom koje se izlaz dovodi u stanje logičke jedinice - faza punjenja izlaznih kapacitivnosti (*precharge*), izvršna (*evaluation*) faza tokom koje izlaz dobija željenu vrednost i faza pražnjenja kondenzatora (*discharge*),

tokom koje se izlazni signal dovodi u stanje logičke nule. Prednost ovog metoda u odnosu na nešto stariji metod WDDL [6-7] ogleda se u imunosti na neuparenost opterećenja na pravom i lažnom izlazu. Ovo je postignuto primenom dinamičkog NOR kola (Dnor) kojim se minimizuje uticaj struje kratkog spoja u CMOS kolu. Ono je sastavni deo kako kontrolne logike tako i samih ćelija i prikazano je na Sl. 1. Slika 2 predstavlja talasne oblike kontrolnih signala Dnor ćelije.

Tokom pripremne faze (PRE) signali *Pre* i *Dis* su u stanju logičke 0. Time se izlaz (*Out*) dovodi u stanje logičke jedinice, nezavisno od stanja ulaznog signala *IN*. Izvršna faza (EVALUATION) počinje kada signal *Pre* dostigne logičku jedinicu. Tada se na izlazu ostvaruje funkcija invertovanja ulaznog signala. Faza pražnjenja (DIS) nastaje kada su signali *Pre* i *Dis* u stanju logičke jedinice. Dakle, tokom pripremne faze izlazni signal uvek uzima visoki, a tokom faze pražnjenja niski logički nivo. Sve ovo može se videti u Tabeli I.



Sl. 1. Prikaz Dnor ćelije



Sl. 2. Talasni oblici kontrolnih signala Dnor ćelije

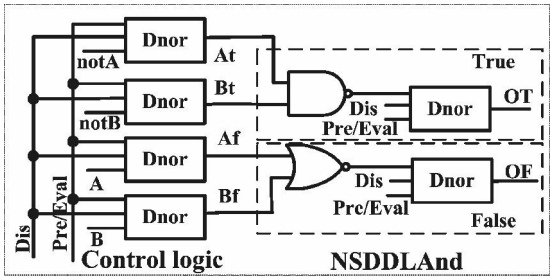
TABELA I
LOGIČKA FUNKCIJA DNOR ĆELIJE

	Signali			
Faze	Pre	Dis	In	Out
Precharge	0	0	0/1	1
Evaluation	1	0	0/1	1/0
Discharge	1	1	0/1	0

III. TESTIRANJE NSDDL AND ĆELIJE

U ovom poglavlju prvo ćemo se osvrnuti na projektovanje NSDDL AND/NAND/OR/NOR ćelije [8-9]. Ista hardverska struktura obezbeđuje funkcije AND, NAND, OR i NOR u zavisnosti od rasporeda ulaznih i izlaznih portova i na taj način mogu se obezbediti četiri različite funkcije istom ćelijom. Sve funkcije ostvaruju se korišćenjem osnovnih kola sa negativnom logikom (NAND i NOR) čija je realizacija u CMOS tehnici izuzetno racionalna.

Slika 3 prikazuje NSDDL AND/NAND/OR/NOR hardversku strukturu sa rasporedom ulaznih portova kojim se realizuje AND funkcija. Deo ćelije u kome se ostvaruje prava vrednost signala označen je sa True, dok je se lažna vrednost signala generiše u potkolu označenom kao False. Na Sl. 3 oni su uokvireni isprekidanim linijama. Pravi i lažni izlazi označeni su sa *OT* i *OF*, respektivno. Posmatranjem ovih blokova može se videti da su to dve komplementarne strukture gde *OT* zavisi od ulaznih signala *At* i *Bt*, a *OF* od *Af* i *Bf* ulaznih signala.



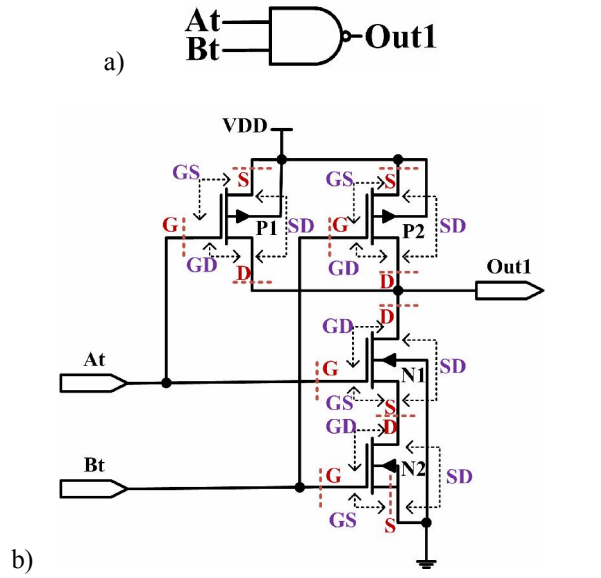
Sl. 3. Blok dijagram NSDDL AND ćelije

Bitno je reći da se osnovni način zaštite od DPA sastoji u razbijanju korelacije između aktivnosti kola i potrošnje. Što je korelacija veća to je kolo ranjivije. Posmatranjem struje I_{DD} cela informacija, o stanju na izlazu, postaje prepoznatljiva i dostupna ukoliko kolo nije dovoljno zaštićeno. Upravo iz ovih razloga kao osnovni pokazatelj o skrivenosti informacija posmatra se dinamička potrošnja kola. Dinamička potrošnja energije iskazana je kroz integral snage ($I_{DD} \cdot V_{DD}$), odnosno struje napajanja (I_{DD}) tokom jednog ciklusa promene ulaznih signala. Za standardnu AND ćeliju ovaj ciklus obuhvata isti vremenski interval kao i za NSDDL ćeliju u sve tri faze rada pri istim ulaznim signalima. Kao mera otpornosti digitalne ćelije na bočne napade usvojen je *NSD* parametar koji predstavlja standardnu devijaciju energije normalizovanu sa prosečnom potrošnjom energije. Kod standardne AND ćelije ovaj parametar iznosi 83.91% dok kod kriptovane NSDDL AND ćelije ovaj parametar je drastično manji i iznosi 0.87%. Postignuta je značajna uniformnost potrošnje koja ovu ćeliju kvalifikuje kao otpornu na bočne napade DPA tipa. Dalje u radu vrednost ovog parametra kriptovane ćelije biće korišćen prilikom poređenja ispravne ćelije i ćelije sa defektom.

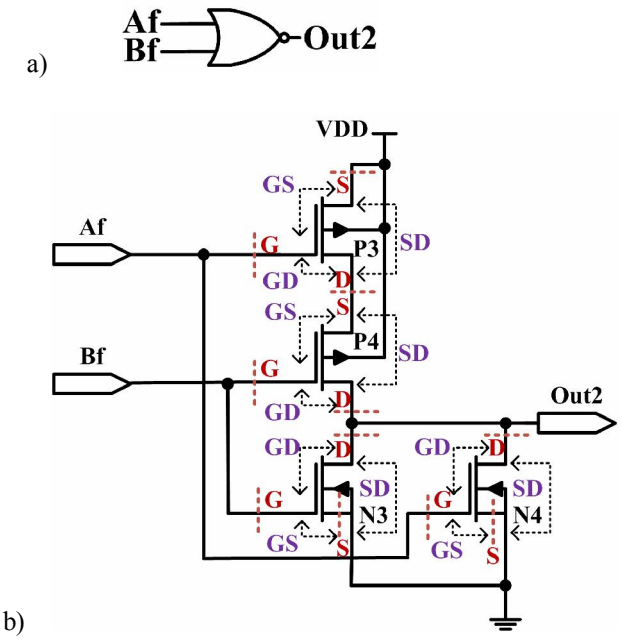
Slika 4a prikazuje standardnu NAND ćeliju u vidu simbola dok slika 4b daje prikaz iste ćelije na šematskom nivou (preuzeta iz TSMC035u biblioteke [12]) sa označenim defektima koji se modeluju. Ista analogija primenjena je i za NOR ćeliju, što se može videti na slikama 5a i 5b. Tranzistori su označeni sa P_i ili N_j, gde P i N predstavljaju tipove tranzistora. Brojači označeni kao i=1-4 i j=1-4 predstavljaju indekse za PMOS i NMOS tranzistore, respektivno.

Da bi se kreirao rečnik defekata [10] neophodno je, za početak, odrediti skup defekata koji se testiraju. Nakon toga,

potrebno je uneti defekte u kolo, i to jedan za drugim, kako bi se analizirao uticaj određenog defekta na funkciju kola.



Sl. 4. Standardna NAND ćelija a) Simbol b) standardna CMOS realizacija sa označenim defektima



Sl. 5. Standardna NOR ćelija a) Simbol b) standardna CMOS realizacija sa označenim defektima

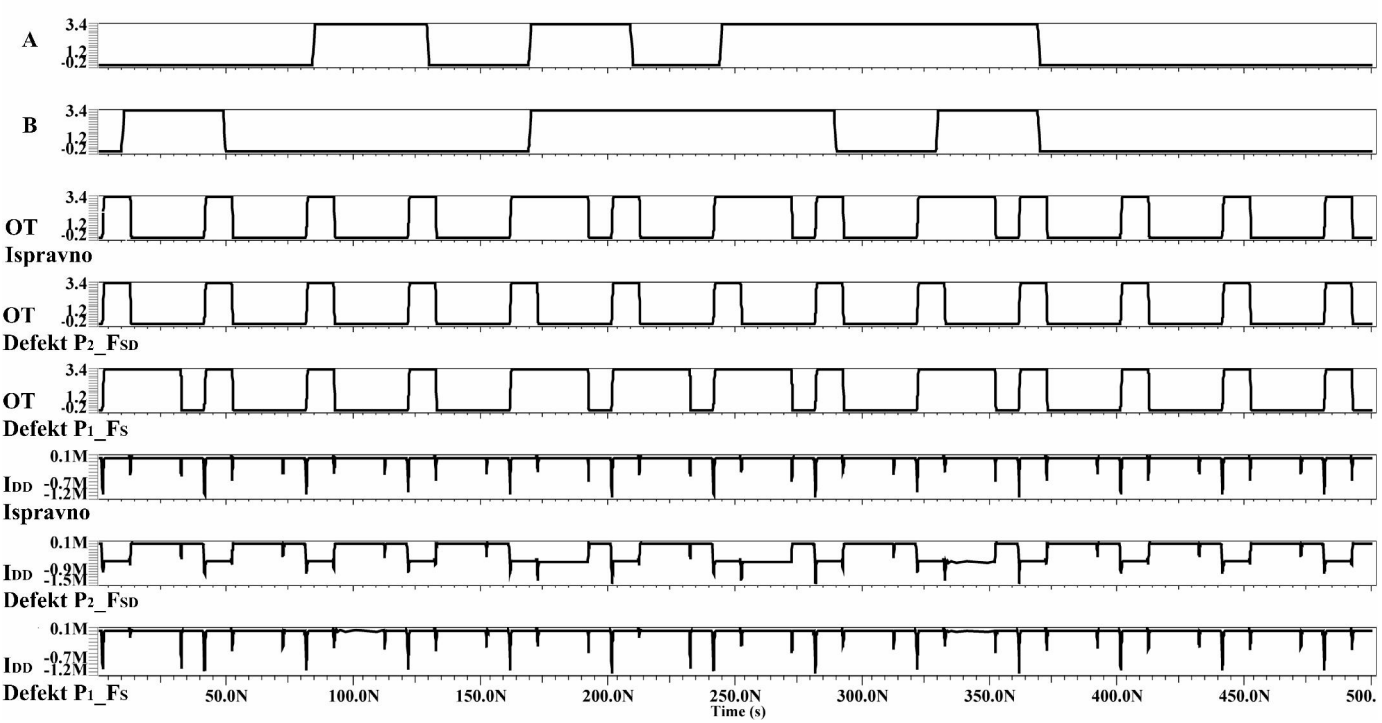
TABELA II
POKRIVENOST DEFEKATA ZA TRUE POTKOLO

	Vrednosti signala												$NSD_{NSDDL\ AND}$
Ispravno kolo													
At	**0**	**0**	**1**	**0**	**1**	**0**	**1**	**1**	**1**	**0**	**0**	**0**	**NA**
Bt	**1**	**0**	**0**	**0**	**1**	**1**	**1**	**0**	**1**	**0**	**0**	**0**	**NA**
OT	**0**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0.87**
OT u prisustvu defekta tipa kratak spoj													
$P_1\_F_{GD}$	↓	0	0	0	0	↓	0	0	0	0	0	0	31.64
$P_1\_F_{GS}$	1	0	0	0	1	1	1	0	1	0	0	0	54.11
$P_1\_F_{SD}$	0	0	0	0	0	0	0	0	0	0	0	0	53.64
$P_2\_F_{GD}$	0	0	↓	0	0	0	0	↓	0	0	0	0	29.54
$P_2\_F_{GS}$	0	0	1	0	1	0	1	1	1	0	0	0	54.11
$P_2\_F_{SD}$	0	0	0	0	0	0	0	0	0	0	0	0	53.64
$N_1\_F_{GD}$	↓	0	0	0	0	↓	0	0	0	0	0	0	31.67
$N_1\_F_{GS}$	0	0	0	0	0	0	0	0	0	0	0	0	0.48
$N_1\_F_{SD}$	↓	0	0	0	1	↓	1	0	1	0	0	0	151.0
$N_2\_F_{GD}$	0	0	0	0	0	0	0	0	0	0	0	0	37.28
$N_2\_F_{GS}$	0	0	0	0	0	0	0	0	0	0	0	0	0.50
$N_2\_F_{SD}$	0	0	↓	0	1	0	1	↓	1	0	0	0	151.2
OT u prisustvu defekta tipa prekid													
$P_1\_F_G$	0	0	0	0	0	0	0	0	0	0	0	0	53.02
$P_1\_F_S$	1	0	0	0	1	1	1	0	1	0	0	0	0.45
$P_1\_F_D$	1	0	0	0	1	1	1	0	1	0	0	0	0.89
$P_2\_F_G$	0	0	0	0	0	0	0	0	0	0	0	0	52.82
$P_2\_F_S$	0	0	1	0	1	0	1	1	1	0	0	0	0.77
$P_2\_F_D$	0	0	1	0	1	0	1	1	1	0	0	0	0.89
$N_1\_F_G$	0	0	0	0	0	0	0	0	0	0	0	0	0.79
$N_1\_F_S$	0	0	0	0	0	0	0	0	0	0	0	0	0.49
$N_1\_F_D$	0	0	0	0	0	0	0	0	0	0	0	0	0.91
$N_2\_F_G$	0	0	0	0	0	0	0	0	0	0	0	0	2.66
$N_2\_F_S$	0	0	0	0	0	0	0	0	0	0	0	0	0.72
$N_2\_F_D$	0	0	0	0	0	0	0	0	0	0	0	0	0.49

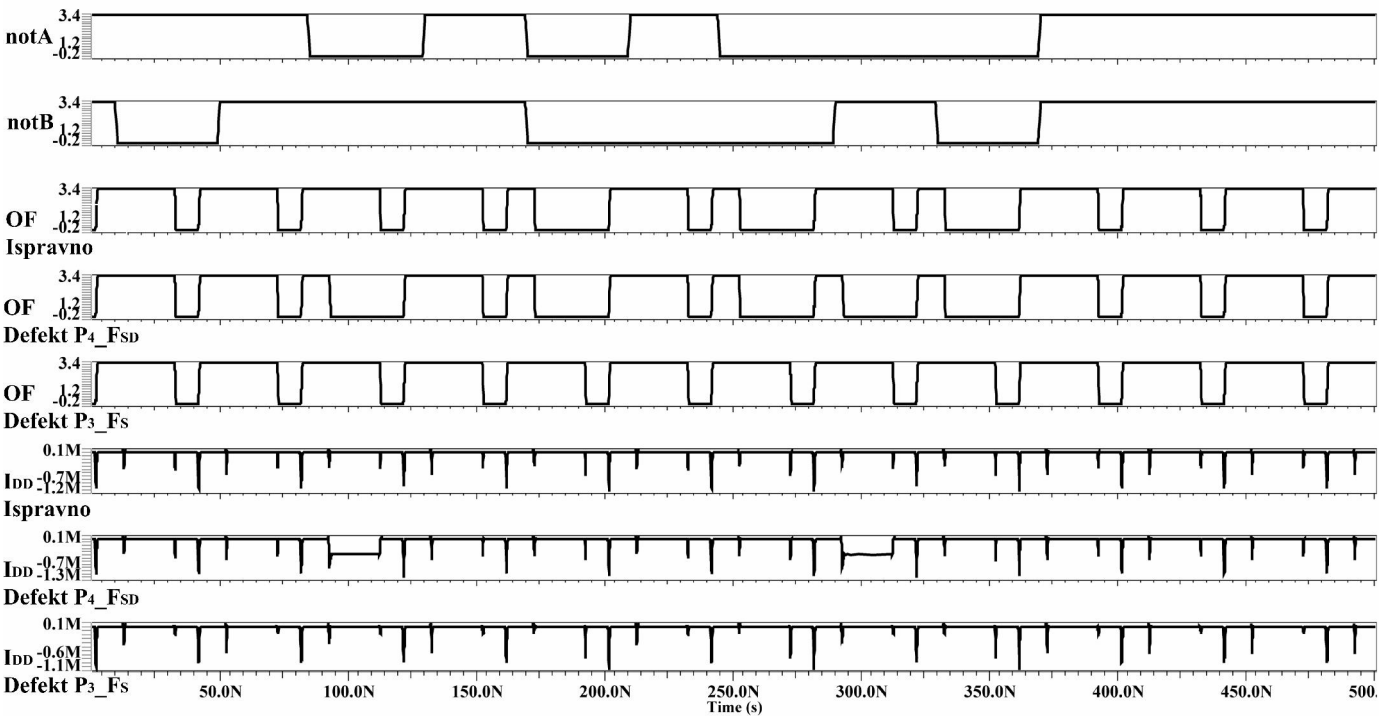
TABELA III
POKRIVENOST DEFEKATA ZA FALSE POTKOLO

	Vrednosti signala												$NSD_{NSDDL\ AND}$
Ispravno kolo													
Af	**1**	**1**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**1**	**1**	**1**	**NA**
Bf	**0**	**1**	**1**	**1**	**0**	**0**	**0**	**1**	**0**	**1**	**1**	**1**	**NA**
OF	**1**	**1**	**1**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**1**	**1**	**0.87**
OF u prisustvu defekta tipa kratak spoj													
$P_3\_F_{GD}$	1	1	1	1	1	1	1	1	1	1	1	1	42.99
$P_3\_F_{GS}$	1	1	1	1	1	1	1	1	1	1	1	1	54.38
$P_3\_F_{SD}$	0	1	1	1	0	0	0	1	0	1	1	1	145.25
$P_4\_F_{GD}$	1	1	0	1	1	1	1	0	1	1	1	1	22.77
$P_4\_F_{GS}$	1	1	1	1	1	1	1	1	1	1	1	1	57.39
$P_4\_F_{SD}$	1	1	0	1	0	1	0	0	0	1	1	1	145.06
$N_3\_F_{GD}$	1	1	0	1	1	1	1	0	1	1	1	1	22.77
$N_3\_F_{GS}$	1	1	0	1	0	1	0	0	0	1	1	1	0.44
$N_3\_F_{SD}$	1	1	1	1	1	1	1	1	1	1	1	1	52.86
$N_4\_F_{GD}$	0	1	1	1	↓	0	↓	1	↓	1	1	1	24.18
$N_4\_F_{GS}$	0	1	1	1	0	0	0	1	0	1	1	1	0.44
$N_4\_F_{SD}$	1	1	1	1	1	1	1	1	1	1	1	1	52.86
OF u prisustvu defekta tipa prekid													
$P_3\_F_G$	↓	1	1	1	0	↓	0	1	0	1	1	1	126.74
$P_3\_F_S$	1	1	1	1	1	1	1	1	1	1	1	1	0.79
$P_3\_F_D$	1	1	1	1	1	1	1	1	1	1	1	1	0.72
$P_4\_F_G$	1	1	↓	1	0	1	0	↓	0	1	1	1	139.51
$P_4\_F_S$	1	1	1	1	1	1	1	1	1	1	1	1	0.72
$P_4\_F_D$	1	1	1	1	1	1	1	1	1	1	1	1	1.12
$N_3\_F_G$	1	1	1	1	0	1	0	1	0	1	1	1	1.61
$N_3\_F_S$	1	1	1	1	0	1	0	1	0	1	1	1	1.24
$N_3\_F_D$	1	1	1	1	0	1	0	1	0	1	1	1	1.57
$N_4\_F_G$	1	1	1	1	0	1	0	1	0	1	1	1	1.20
$N_4\_F_S$	1	1	1	1	0	1	0	1	0	1	1	1	0.66
$N_4\_F_D$	1	1	1	1	1	1	1	1	1	1	1	1	1.02

Defekti mogu biti svrstani u dve kategorije. Prva bi označavala katastrofalne defekte u koje se ubrajaju kratak spoj i prekid u kolu, dok se defekti parametarskog tipa svrstavaju u kategoriju mekih defekata. U radu [11] predstavljeni su rezultati za podgrupu katastrofalnih defekata i to tipa kratak spoj. Ovde prikazujemo rezultate koji dopunjuju grupu katastrofalnih defekata dodavanjem podgrupe defekata tipa prekid. Na ovaj način biće formiran potpuni rečnik katastrofalnih defekata za NSDDL AND ćeliju. Efekat svakog defekta najpre je posmatran sa strane narušavanja logičke funkcije kola. Kada se naruši logička funkcija kola, to automatski označava da je defekt u kolu detektabilan. Ovaj način sagledanja rezultata simulacije u velikoj meri je omogućio detektovanje defekata u kolu. Tabela II daje rezultate za True potkolo dok se Tabela III odnosi na False potkolo.



Sl. 6. TRUE potkolo - Poređenje talasnih oblika napona i struje ispravnog i kola sa defektom tipa kratak spoj(P_2_F_{SD}) odnosno prekid (P_1_F_S)



Sl. 7. FALSE potkolo - Poređenje talasnih oblika napona i struje ispravnog i kola sa defektom tipa kratak spoj(P_4_F_{SD}) odnosno prekid (P_3_F_S)

Tipovi defekata označeni su sa $P_i\_F_{xy}$ ili $N_j\_F_{xy}$, gde P_i i N_j predstavljaju tipove tranzistora; F_{xy} označava defekt kratkog spoja između x i y priključaka odgovarajućeg tranzistora. Kombinacije xy mogu biti GD (gejt-drejn), GS (gejt-sors) ili SD (sors-drejn); F_x označava defekt prekida, gde x može uzeti vrednost G(gejt), D(drejn) ili S(sors). Simbol "↓" označava prelazno stanje sa 1 na 0. Posmatrajući rezultate iz ove dve tabele može se videti da su detektabilni svi defekti za koje postoji razlika u logičkoj funkciji kola ili u *NSD* parametru ili oba. Kako je funkcija ovog kola specifična, usled primene NSDDL metoda, prava vrednost signala se pojavljuje u toku trajanja *EVALUATION* faze. Vrednosti izlaznih signala iz Tabela II i III su one koje se javljaju u pomenutoj fazi.

Slike 6 i 7 predstavljaju bitne talasne oblike za True i False potkola, respektivno. Razlike talasnih oblika odziva i struje napajanja ispravnog kola i kola sa defektom indicira efekat njegovog delovanja. Za True potkolo posmatrani su efekti defekata tipa kratak spoj $P_2\_F_{SD}$ odnosno prekid $P_1\_F_S$, dok su za False potkolo prikazani efekti defekata tipa kratak spoj $P_4\_F_{SD}$ odnosno prekid $P_3\_F_S$. Može se videti da je svaki posmatrani defekt utisnut kako u odziv kola tako i u struju napajanja. Kada se pogledaju Tabele II i III i vrednost *NSD* parametara, za pomenute defekte, jasno se može videti njihov uticaj i po ovom kriterijumu. Dakle, testiranje zasnovano na struji napajanja je odličan dodatni izvor informacija pored posmatranog odziva kola. Za svaki testirani defekt proračunat je i *NSD* parametar kao drugi indikator. Male promene ovog parametra ukazuju na neku nepravilnost u kolu što se može videti u pomenutim tabelama. Logičkom funkcijom kola detektovano je 89.53% defekata. Defekti koji nisu detektovani logičkom funkcijom su: $N_3\_F_G$, $N_3\_F_S$, $N_3\_F_D$, $N_4\_F_G$ $N_4\_F_S$ iz Tabele III. Međutim kada se pogleda *NSD* parametar za navedene defekte, jasno je da u kolu postoji neka nepravilnost. Ravnopravnim posmatranjem oba pokazatelja pokrivenost defekata je 100% ostvarena.

IV. Zaključak

NSDDL metod primenjen u projektovanju digitalnih ćelija otpornih na bočne napade. Zasnovan je na ideji da se pri svakoj kombinaciji ulaznih signala ostvari ista potrošnja energije. Ovo je moguće u slučaju da se osim regularnog izlaza uvede i komplementarni, odnosno lažni izlazni signal. Praktično to znači da se originalnoj ćeliji pridružuje ćelija sa komplementarnim svojstvima. Time se duplira hardver, ali se ostvaruje efekat razbijanja korelacije između funkcije ćelije i potrošnje.

Za testiranje NSDDL AND ćelije usvojena su dva kriterijuma: potvrda logičke funkcije kola kao i I_{DDQ} testiranje iskazano kroz *NSD* parametar. Izvedeno je četrdeset osam simulacija i kreiran je odgovarajući rečnik defekata za defekte tipa kratak spoj i prekid u kolu. Nakon kompletnog sumiranja može se reći da su dobijeni rezultati očekivani. Kada se posmatraju oba kriterijuma može se reći da je pokrivenost defekata potpuna jer je svih četrdeset osam defekata detektovano. Simetrija, koja je ključna u ovakvom načinu projektovanja, je porušena pa efekat defekta odmah postaje vidljiv na izlazu ćelije, struji napajanja ili oba. Važno je napomenuti da se istim hardverom ostvaruju i NAND, OR, i NOR funkcije u NSDDL logici, tako da izvedeni zaključci važe za sve ove ćelije.

Zahvalnica

Rezultati prikazani u ovom radu ostvareni su u okviru projekta TR 32004 koji je finansiran od strane Ministarstva prosvete, nauke i tehnološkog razvoja Republike Srbije.

Literatura

[1] V. Lomné, A. Dehaboui, P. Maurine, L. Torres, M. Robert, "Side Channel Attack"', in B. Badrignans, J. L. Danger, V. Fischer, G. Gogniat, L. Torres, "Security Trends for FPGA", Springer Netherlands 2011, pp. 47-72.

[2] J. J.Quisquater, "Side channel attacks", State-of-the-Art, Rep, October 2002.

[3] L. Sauvage, S. Guilley and Y. Mathieu, "ElectroMagnetic radiations of FPGAs: high spatial resolution cartography and attack of a cryptographic module", ACM Transactions on Reconfigurable Technology and Systems, 2009, vol. 2, no. 1, pp. 1-24.

[4] J. Quan and G.Bai, "A new method to reduce the side-channel leakage caused by unbalanced capacitances of differential interconnections in dual rail logic styles", Sixth International Conference on Information Technology: New Generations, 2009, pp. 58-63.

[5] B. Milovanović., and V. Litovski, "Fault models of CMOS Circuits", Microelectronics Reliability, Vol. 34, No. 5, pp. 883-896, 1994.

[6] K. Tiri and I. Verbauwhede, "A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation", in Proc. Design, Automation and Test in Europe, IEEE Computer Society, Feb 2004, pp. 246-251.

[7] K. Tiri and I. Verbauwhede, "Place and Route for Secure Standard Cell Design", CARDIS'04, pp. 143-158, 2004.

[8] M. Stanojlović,„P. Petković: *„An ASIC cryptoosystem resistant to side channel attacks based on standard cells"*, VIII Simposium on Industrial Electronics INDEL 2010, Banja Luka, Bosnia and Herzegovina, 4-6 November, 2010, pp. 110-114, ISBN 978-99955-46-03-8, In Serbian

[9] P. Petković, M. Stanojlović: „*Hardware protection from side channel attacks based on masking the consumption information"*, Zbornik LV konferencije ETRAN, Banja Vrućica, Teslić, B&H, 2011, ISBN 978-86-80509-66-2

[10] V. Litovski, "Osnovi testiranja elektronskih kola", Elektronski fakultet, Niš, ISBN 978-86-85195-71-6, 2009

[11] M. Stanojlović, V. Litovski, P. Petković: „*Testing an SCA hardened combinational standard cell - preliminary considerations"*,Proceedings of the 5th Small System Simulation Symposium, Niš, 2014, ISBN 978-86-6125-098-9

[12] ASIC Design Kit, (http://www.mentor.com/company/higher_ed/ic-asic)

Abstract

In this paper results of testing an NSDDL AND cell that is part of NSDDL (No Short-circuit current Dynamic Differential Logic) side-channel-attack-resistant library will be presented. Fault dictionary will be created based on repetitive simulation preformed for defects inserted one by one. Verification will show the degree of vulnerability AND logic cell in the presence of defects. For a short and open circuit defects detection logical function and supply current will be exploited. The cell is designed in CMOS TSMC035 technology using Mentor Graphics design tools.

Testing an SCA hardened combinational standard AND cell

Milena Stanojlović, Vančo Litovski, Predrag Petković